Faculty of Engineering, Computing and Science

COS20030 Malware Analysis

Skills Test Lab 1 (10 marks)

Fill in the particulars for your team below.

	Student Name	**Student ID**
1	Chin Chun Kiat	102765068
2	Chong Chao Sen	102762412
3		

General Instructions to Students

1. Skills Test Lab 1 is worth 10% of the unit's grade.
2. You are given a duration of 1 hour 30 minutes to complete the test.
3. Sign-in to Canvas before starting the test. Download the test question and any materials needed for the test. You will be using the VM that you normally use for the weekly labs.
4. List of things that are NOT ALLOWED during the test:
    a. Not allowed to communicate with other teams: You are only allowed to collaborate with your teammate from the same group.
    b. Usage of mobile phone is only allowed for 2FA authentication when signing-in to Canvas. After that, you must place your mobile phone in your bag, and your bag should be placed on the floor below your table. In case of exceptional circumstances where you need to use your mobile phone, you may ask the invigilator for approval.
    c. Not allowed to run any instant communication applications on your computer such as WhatsApp, Teams, Discord, etc.
5. You have only ONE submission attempt in Canvas. Check your document properly before submit.
    a. Only document in PDF format is accepted.
    b. Only 1 group member need to submit on behalf of the team.
    c. You won't be able to view your Turnitin score. It is only visible to the tutor.
    d. You must leave the hall immediately after completing your submission in Canvas.
6. After the test has ended, no resubmission is allowed.

Marking Criteria

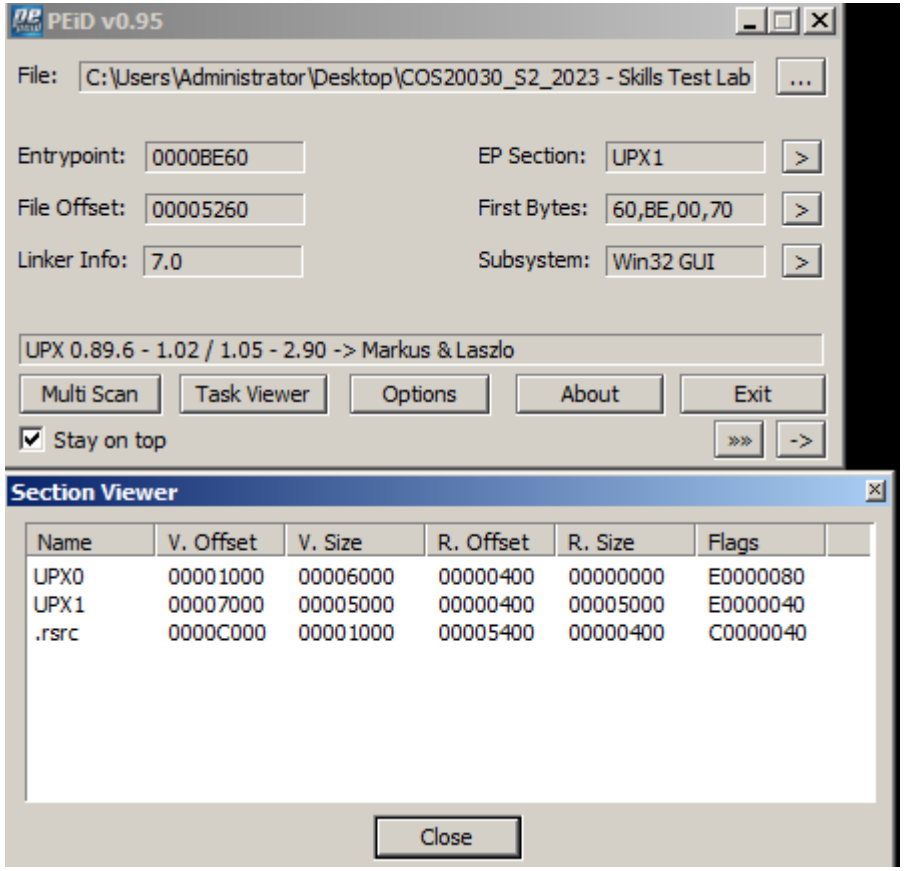
Question	Standards achieved		
Q1	**6 marks** Utilised all the static analysis tools available. Indicators are described and explained with a high level of detail. Demonstrated capability to explore or research for more information	**4 marks** Utilised all the static analysis tools available. Indicators are described and explained well.	**2 marks** Limited usage of the static analysis tools. Minimal description/ explanation on the indicators.
Q2	**4 marks** Utilised all specified dynamic analysis tools. Indicators are described/ explained with a high level of detail. Demonstrated capability to explore or research for more information	**3 marks** Utilised all specified dynamic analysis tools. Indicators are described/ explained well.	**1 marks** Limited usage of specified dynamic analysis tools. Minimal description/ explanation on the indicators.

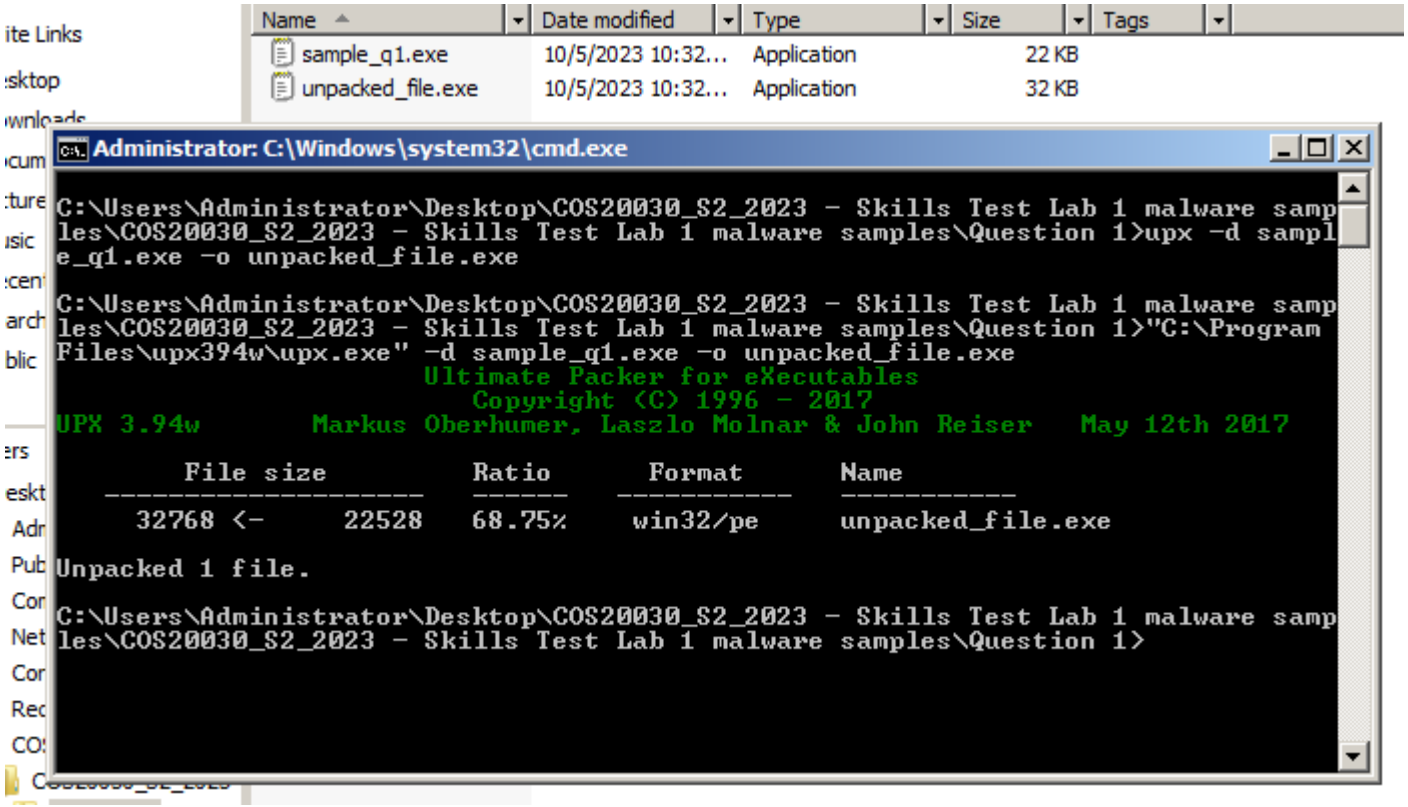
Question 1

As a malware analyst, you are given a suspicious file named "sample_q1.exe" to investigate. Using the tools you have learned in the weekly labs, you are required to perform *static analysis* on these files.

Document your findings in the table below. Include screenshots where necessary.

Filename: sample_q1.exe		
Criteria	**Description/explanation**	**Tool used**

Indicator that the file is packed	 It is a packed file that the EP section shown that it is UPX1 which is a most known packer that helps to mask malware.	PeiD, Command Prompt



By using the command “upx -d sample_q1.exe -o unpacked_file.exe”, the user unpacked the file and named it unpacked_file.exe

File imports	1) Using Dependency Walker: UNPACKED_FILE.EXE KERNEL32.DLL ADVAPI32.DLL MSVCRT.DLL USER32.DLL WS2_32.DLL	Dependency Walker, Peview, VirusTotal

There are five libraries found.

a) Functions in KERNEL32.DLL:

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	0 (0x0000)	CreateFileMappingA	Not Bound
C	N/A	0 (0x0000)	FindNextFileA	Not Bound
C	N/A	0 (0x0000)	FindFirstFileA	Not Bound
C	N/A	0 (0x0000)	GetEnvironmentVariableA	Not Bound
C	N/A	0 (0x0000)	GetWindowsDirectoryA	Not Bound
C	N/A	0 (0x0000)	GetDriveTypeA	Not Bound
C	N/A	0 (0x0000)	GetFileSize	Not Bound
C	N/A	0 (0x0000)	FindClose	Not Bound
C	N/A	0 (0x0000)	FileTimeToSystemTime	Not Bound
C	N/A	0 (0x0000)	GetTempFileNameA	Not Bound
C	N/A	0 (0x0000)	SetFilePointer	Not Bound
C	N/A	0 (0x0000)	GetSystemTime	Not Bound
C	N/A	0 (0x0000)	GetCurrentThread	Not Bound
C	N/A	0 (0x0000)	WriteFile	Not Bound
C	N/A	0 (0x0000)	LoadLibraryA	Not Bound
C	N/A	0 (0x0000)	lstrcpyA	Not Bound
C	N/A	0 (0x0000)	CloseHandle	Not Bound
C	N/A	0 (0x0000)	GetFileAttributesA	Not Bound
C	N/A	0 (0x0000)	CreateFileA	Not Bound
C	N/A	0 (0x0000)	lstrlenA	Not Bound
C	N/A	0 (0x0000)	GetTempPathA	Not Bound
C	N/A	0 (0x0000)	GetSystemDirectoryA	Not Bound
C	N/A	0 (0x0000)	lstrcatA	Not Bound
C	N/A	0 (0x0000)	GetLastError	Not Bound
C	N/A	0 (0x0000)	CreateMutexA	Not Bound
C	N/A	0 (0x0000)	CopyFileA	Not Bound
C	N/A	0 (0x0000)	DeleteFileA	Not Bound
C	N/A	0 (0x0000)	SetFileAttributesA	Not Bound
C	N/A	0 (0x0000)	GetModuleFileNameA	Not Bound
C	N/A	0 (0x0000)	SystemTimeToFileTime	Not Bound
C	N/A	0 (0x0000)	GetSystemTimeAsFileTime	Not Bound
C	N/A	0 (0x0000)	Sleep	Not Bound
C	N/A	0 (0x0000)	ExitThread	Not Bound
C	N/A	0 (0x0000)	WaitForSingleObject	Not Bound
C	N/A	0 (0x0000)	CreateProcessA	Not Bound

C	N/A	0 (0x0000)	CreateThread	Not Bound
C	N/A	0 (0x0000)	GetTickCount	Not Bound
C	N/A	0 (0x0000)	ExitProcess	Not Bound
C	N/A	0 (0x0000)	GetTimeZoneInformation	Not Bound
C	N/A	0 (0x0000)	MapViewOfFile	Not Bound
C	N/A	0 (0x0000)	FileTimeToLocalFileTime	Not Bound
C	N/A	0 (0x0000)	GetLocalTime	Not Bound
C	N/A	0 (0x0000)	WideCharToMultiByte	Not Bound
C	N/A	0 (0x0000)	GetProcAddress	Not Bound
C	N/A	0 (0x0000)	GetModuleHandleA	Not Bound
C	N/A	0 (0x0000)	HeapFree	Not Bound
C	N/A	0 (0x0000)	GetProcessHeap	Not Bound
C	N/A	0 (0x0000)	HeapAlloc	Not Bound
C	N/A	0 (0x0000)	lstrcpynA	Not Bound
C	N/A	0 (0x0000)	lstrcmpA	Not Bound
C	N/A	0 (0x0000)	lstrcmpiA	Not Bound
C	N/A	0 (0x0000)	GlobalFree	Not Bound
C	N/A	0 (0x0000)	InterlockedDecrement	Not Bound
C	N/A	0 (0x0000)	InterlockedIncrement	Not Bound
C	N/A	0 (0x0000)	ReadFile	Not Bound
C	N/A	0 (0x0000)	UnmapViewOfFile	Not Bound
C	N/A	0 (0x0000)	SetThreadPriority	Not Bound

- File management tasks like generating, copying, deleting, or inspecting file attributes are all possible uses for functions like CreateFileA, CopyFileA, DeleteFileA, and GetFileAttributesA.
- The code may be reading from or writing to files if it uses functions like ReadFile, WriteFile, and SetFilePointer for file I/O operations.
- The code may deal with creating and managing processes and threads, as suggested by functions like CreateProcessA, CreateThread, WaitForSingleObject, and Sleep.
- Task timing and scheduling can be accomplished using GetTickCount and GetSystemTime.
- GlobalAlloc, GlobalFree, HeapAlloc, and HeapFree are examples of memory allocation and deallocation routines that show the code may support memory managemen

b) Functions in ADVAPI32.DLL

PI	Ordinal ^	Hint	Function	Entry Poir
C	N/A	0 (0x0000)	RegCloseKey	Not Bounc
C	N/A	0 (0x0000)	RegOpenKeyExA	Not Bounc
C	N/A	0 (0x0000)	RegSetValueExA	Not Bounc
C	N/A	0 (0x0000)	RegQueryValueExA	Not Bounc
C	N/A	0 (0x0000)	RegEnumKeyA	Not Bounc
C	N/A	0 (0x0000)	RegCreateKeyExA	Not Bounc

- The use of the Windows Registry by the code is implied by functions like RegOpenKeyExA, RegSetValueExA, RegQueryValueExA, and RegCloseKey, which may be used to store configuration or settings.

c) Functions in MSVCRT.DLL:

PI	Ordinal ^	Hint	Function
C	N/A	0 (0x0000)	memset
C	N/A	0 (0x0000)	tolower
C	N/A	0 (0x0000)	memcpy
C	N/A	0 (0x0000)	isdigit
C	N/A	0 (0x0000)	toupper
C	N/A	0 (0x0000)	isxdigit
C	N/A	0 (0x0000)	isalnum
C	N/A	0 (0x0000)	isspace

- Processes from USER32 that manipulate strings include lstrcpyA, lstrlenA, lstrcatA, and related routines.When working with text data, DLL are frequently utilized.

d) Functions in USER32.DLL:

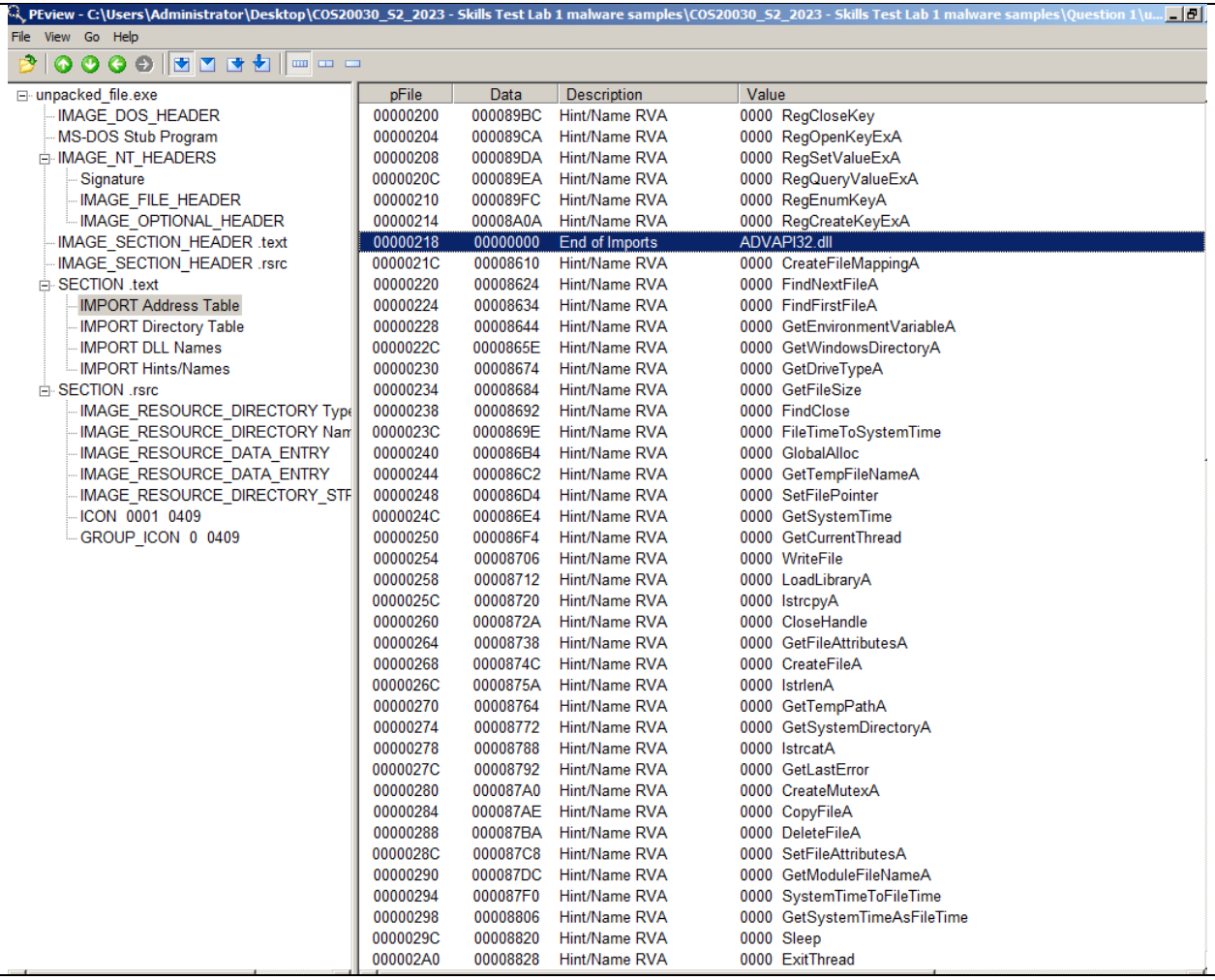
PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	0 (0x0000)	CharUpperBuffA	Not Bound
C	N/A	0 (0x0000)	CharUpperA	Not Bound
C	N/A	0 (0x0000)	CharLowerA	Not Bound
C	N/A	0 (0x0000)	wvsprintfA	Not Bound
C	N/A	0 (0x0000)	wsprintfA	Not Bound

e) Functions in WS2_32.DLL:

PI	Ordinal ^	Hint	Function	Entry Point
0#	3 (0x0003)	N/A	N/A	Not Bound
0#	4 (0x0004)	N/A	N/A	Not Bound
0#	9 (0x0009)	N/A	N/A	Not Bound
0#	10 (0x000A)	N/A	N/A	Not Bound
0#	11 (0x000B)	N/A	N/A	Not Bound
0#	15 (0x000F)	N/A	N/A	Not Bound
0#	16 (0x0010)	N/A	N/A	Not Bound
0#	18 (0x0012)	N/A	N/A	Not Bound
0#	19 (0x0013)	N/A	N/A	Not Bound
0#	20 (0x0014)	N/A	N/A	Not Bound
0#	23 (0x0017)	N/A	N/A	Not Bound
0#	52 (0x0034)	N/A	N/A	Not Bound
0#	111 (0x006F)	N/A	N/A	Not Bound
0#	115 (0x0073)	N/A	N/A	Not Bound
0#	151 (0x0097)	N/A	N/A	Not Bound

The functions cannot be viewed.

2) Using Peview



pFile	Data	Description	Value
00000200	000089BC	Hint/Name RVA	0000 RegCloseKey
00000204	000089CA	Hint/Name RVA	0000 RegOpenKeyExA
00000208	000089DA	Hint/Name RVA	0000 RegSetValueExA
0000020C	000089EA	Hint/Name RVA	0000 RegQueryValueExA
00000210	000089FC	Hint/Name RVA	0000 RegEnumKeyA
00000214	00008A0A	Hint/Name RVA	0000 RegCreateKeyExA
00000218	00000000	End of Imports	ADVAPI32.dll
0000021C	00008610	Hint/Name RVA	0000 CreateFileMappingA
00000220	00008624	Hint/Name RVA	0000 FindNextFileA
00000224	00008634	Hint/Name RVA	0000 FindFirstFileA
00000228	00008644	Hint/Name RVA	0000 GetEnvironmentVariableA
0000022C	0000865E	Hint/Name RVA	0000 GetWindowsDirectoryA
00000230	00008674	Hint/Name RVA	0000 GetDriveTypeA
00000234	00008684	Hint/Name RVA	0000 GetFileSize
00000238	00008692	Hint/Name RVA	0000 FindClose
0000023C	0000869E	Hint/Name RVA	0000 FileTimeToSystemTime
00000240	000086B4	Hint/Name RVA	0000 GlobalAlloc
00000244	000086C2	Hint/Name RVA	0000 GetTempFileNameA
00000248	000086D4	Hint/Name RVA	0000 SetFilePointer
0000024C	000086E4	Hint/Name RVA	0000 GetSystemTime
00000250	000086F4	Hint/Name RVA	0000 GetCurrentThread
00000254	00008706	Hint/Name RVA	0000 WriteFile
00000258	00008712	Hint/Name RVA	0000 LoadLibraryA
0000025C	00008720	Hint/Name RVA	0000 lstrcpyA
00000260	0000872A	Hint/Name RVA	0000 CloseHandle
00000264	00008738	Hint/Name RVA	0000 GetFileAttributesA
00000268	0000874C	Hint/Name RVA	0000 CreateFileA
0000026C	0000875A	Hint/Name RVA	0000 lstrlenA
00000270	00008764	Hint/Name RVA	0000 GetTempPathA
00000274	00008772	Hint/Name RVA	0000 GetSystemDirectoryA
00000278	00008788	Hint/Name RVA	0000 lstrcatA
0000027C	00008792	Hint/Name RVA	0000 GetLastError
00000280	000087A0	Hint/Name RVA	0000 CreateMutexA
00000284	000087AE	Hint/Name RVA	0000 CopyFileA
00000288	000087BA	Hint/Name RVA	0000 DeleteFileA
0000028C	000087C8	Hint/Name RVA	0000 SetFileAttributesA
00000290	000087DC	Hint/Name RVA	0000 GetModuleFileNameA
00000294	000087F0	Hint/Name RVA	0000 SystemTimeToFileTime
00000298	00008806	Hint/Name RVA	0000 GetSystemTimeAsFileTime
0000029C	00008820	Hint/Name RVA	0000 Sleep
000002A0	00008828	Hint/Name RVA	0000 ExitThread

pFile	Data	Description	Value
000002A4	00008834	Hint/Name RVA	0000 WaitForSingleObject
000002A8	0000884A	Hint/Name RVA	0000 CreateProcessA
000002AC	0000885A	Hint/Name RVA	0000 CreateThread
000002B0	00008868	Hint/Name RVA	0000 GetTickCount
000002B4	00008876	Hint/Name RVA	0000 ExitProcess
000002B8	00008884	Hint/Name RVA	0000 GetTimeZoneInformation
000002BC	0000889C	Hint/Name RVA	0000 MapViewOfFile
000002C0	000088AC	Hint/Name RVA	0000 FileTimeToLocalFileTime
000002C4	000088C6	Hint/Name RVA	0000 GetLocalTime
000002C8	000088D4	Hint/Name RVA	0000 WideCharToMultiByte
000002CC	000088EA	Hint/Name RVA	0000 GetProcAddress
000002D0	000088FA	Hint/Name RVA	0000 GetModuleHandleA
000002D4	0000890C	Hint/Name RVA	0000 HeapFree
000002D8	00008916	Hint/Name RVA	0000 GetProcessHeap
000002DC	00008926	Hint/Name RVA	0000 HeapAlloc
000002E0	00008932	Hint/Name RVA	0000 lstrcpynA
000002E4	0000893E	Hint/Name RVA	0000 lstrcmpA
000002E8	00008948	Hint/Name RVA	0000 lstrcmpiA
000002EC	00008954	Hint/Name RVA	0000 GlobalFree
000002F0	00008960	Hint/Name RVA	0000 InterlockedDecrement
000002F4	00008976	Hint/Name RVA	0000 InterlockedIncrement
000002F8	0000898C	Hint/Name RVA	0000 ReadFile
000002FC	00008996	Hint/Name RVA	0000 UnmapViewOfFile
00000300	000089A8	Hint/Name RVA	0000 SetThreadPriority
00000304	00000000	End of Imports	KERNEL32.DLL
00000308	00008A1C	Hint/Name RVA	0000 memset
0000030C	00008A24	Hint/Name RVA	0000 tolower
00000310	00008A2E	Hint/Name RVA	0000 memcpy
00000314	00008A36	Hint/Name RVA	0000 isdigit
00000318	00008A40	Hint/Name RVA	0000 toupper
0000031C	00008A4A	Hint/Name RVA	0000 isxdigit
00000320	00008A54	Hint/Name RVA	0000 isalnum
00000324	00008A5E	Hint/Name RVA	0000 isspace
00000328	00000000	End of Imports	MSVCRT.dll
0000032C	00008A68	Hint/Name RVA	0000 CharUpperBuffA
00000330	00008A78	Hint/Name RVA	0000 CharUpperA
00000334	00008A84	Hint/Name RVA	0000 CharLowerA
00000338	00008A90	Hint/Name RVA	0000 wvsprintfA
0000033C	00008A9C	Hint/Name RVA	0000 wsprintfA
00000340	00000000	End of Imports	USER32.dll

00000344	80000013	Ordinal	0013	
00000348	8000000A	Ordinal	000A	
0000034C	80000004	Ordinal	0004	
00000350	8000006F	Ordinal	006F	
00000354	80000097	Ordinal	0097	
00000358	8000000B	Ordinal	000B	
0000035C	80000034	Ordinal	0034	
00000360	80000017	Ordinal	0017	
00000364	80000012	Ordinal	0012	
00000368	80000010	Ordinal	0010	
0000036C	80000003	Ordinal	0003	
00000370	8000000F	Ordinal	000F	
00000374	80000009	Ordinal	0009	
00000378	80000014	Ordinal	0014	
0000037C	80000073	Ordinal	0073	
00000380	00000000	End of Imports	WS2_32.dll	

User could see that at the “Description” have “End of Imports”, that is the function name.

	3) View in VirusTotal	

Imports

— ADVAPI32.dll

RegCloseKey
RegCreateKeyExA
RegEnumKeyA
RegOpenKeyExA
RegQueryValueExA
RegSetValueExA

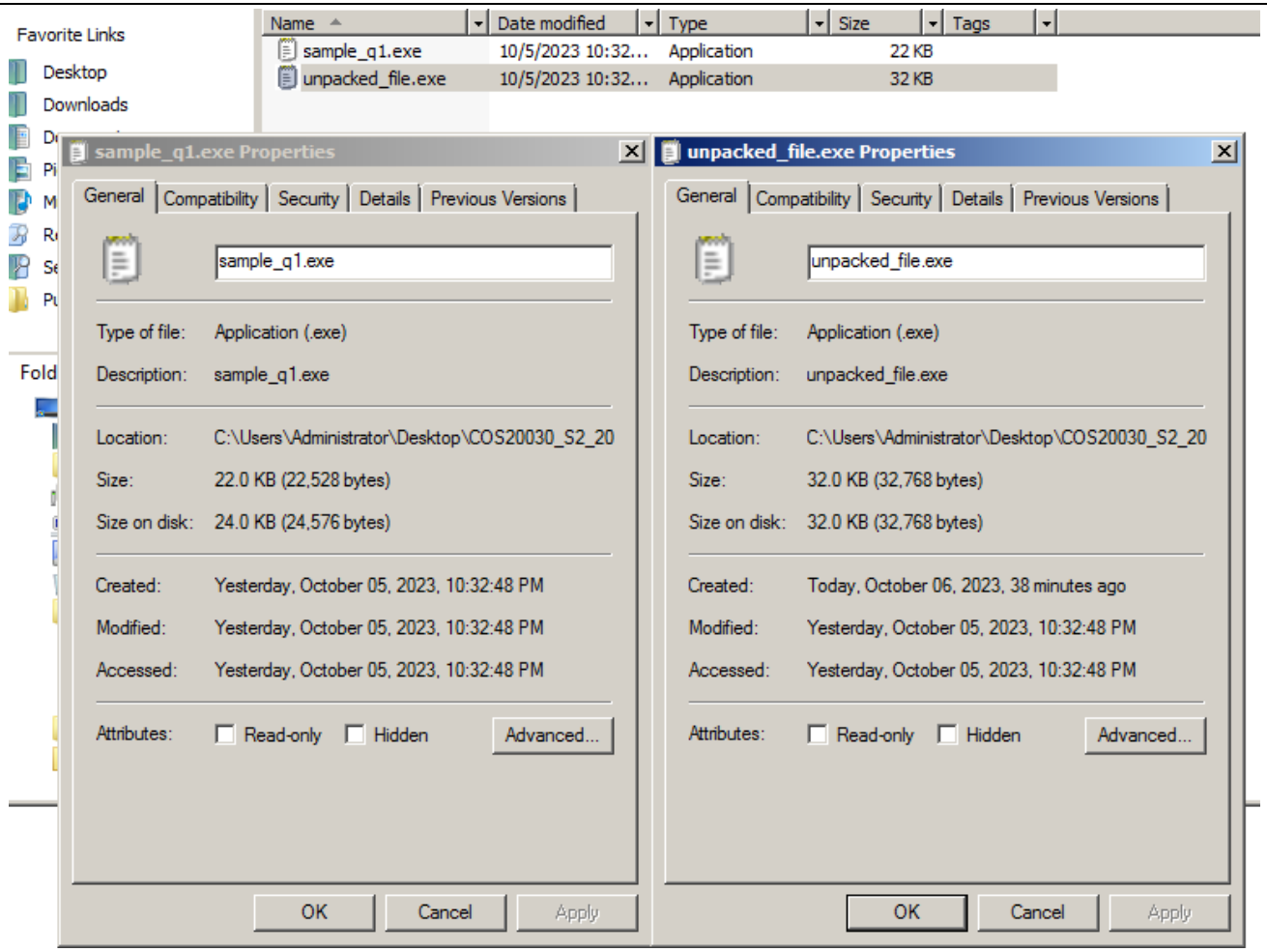
— KERNEL32.DLL

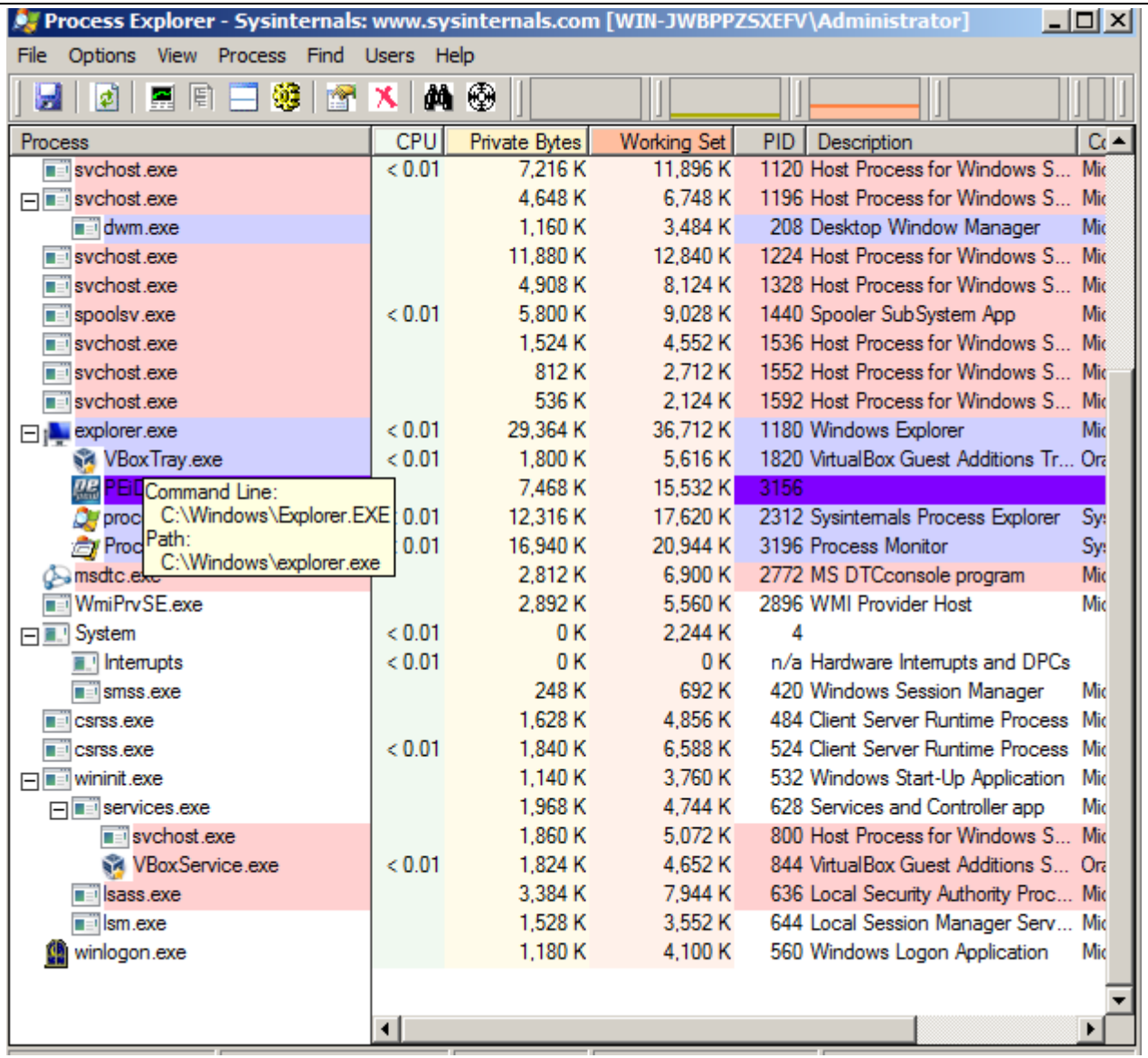
CloseHandle
CopyFileA
CreateFileA
CreateFileMappingA
CreateMutexA
CreateProcessA
CreateThread
DeleteFileA
ExitProcess
ExitThread

— MSVCRT.dll

isalnum
isdigit
isspace
isxdigit
memcpy
memset
tolower
toupper

	— WS2_32.dll __WSAFDIsSet closesocket connect gethostbyname htons inet_addr ioctlsocket ntohs recv select ⌄ — USER32.dll CharLowerA CharUpperA CharUpperBuffA wsprintfA wvsprintfA	

Host-based indicators	 Even though it's a .exe file the icon of the file is like .txt file.	Process Explorer, Process Monitor



After running the unpacked_file.exe of the sample_q1.exe, doesn't seem to saw any running at Process Explorer.

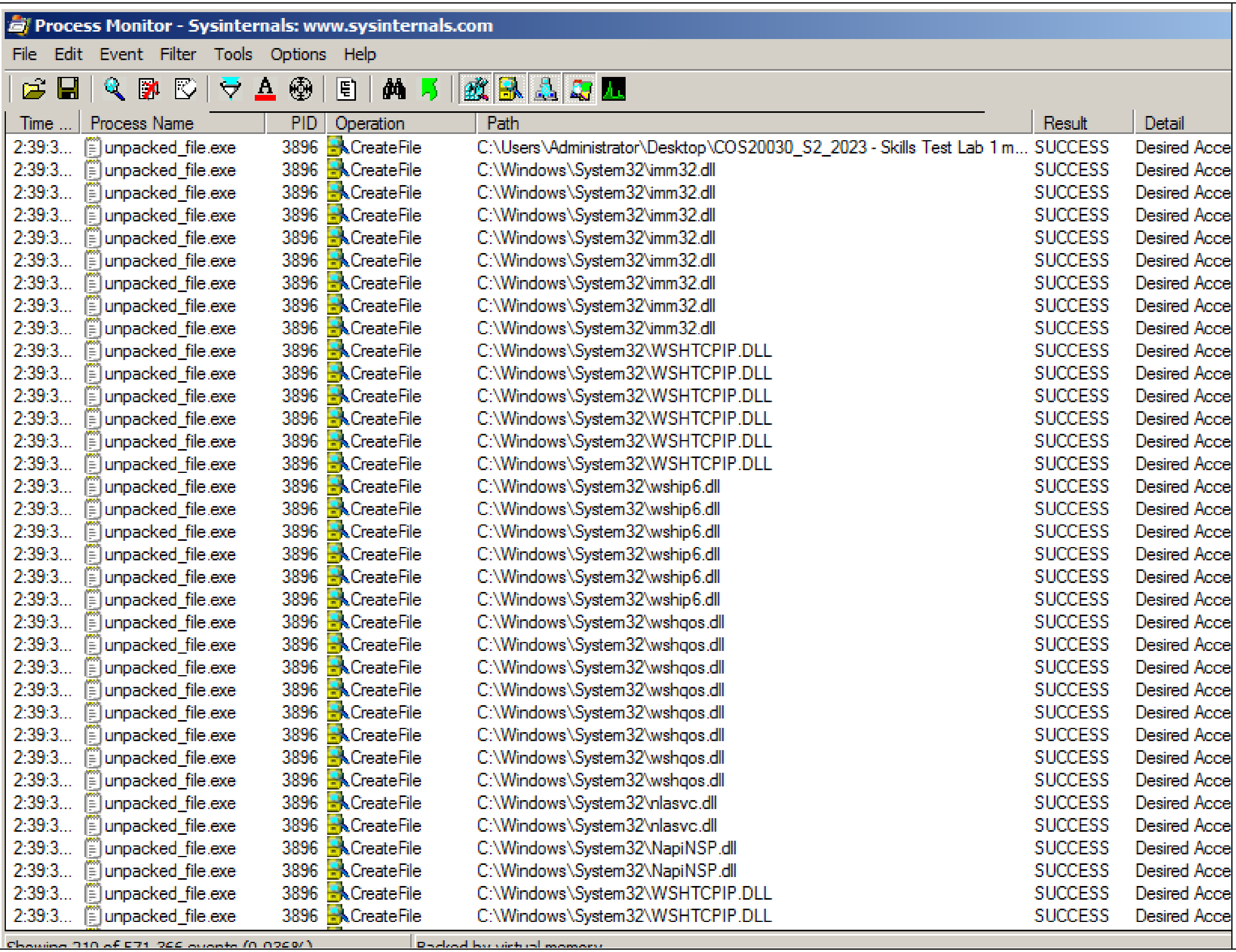
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

Time ...	Process Name	PID	Operation	Path	Result	Detail
2:39:3...	unpacked_file.exe	3896	Process Start		SUCCESS	Parent PID: 1204, Comm...
2:39:3...	unpacked_file.exe	3896	Thread Create		SUCCESS	Thread ID: 3900
2:39:3...	unpacked_file.exe	3896	QueryNameInfo...	C:\Users\Administrator\Desktop\COS20030_S2_2023 - Skills Test Lab 1 m...	BUFFER O...	Name: \Users\Administr...
2:39:3...	unpacked_file.exe	3896	QueryNameInfo...	C:\Users\Administrator\Desktop\COS20030_S2_2023 - Skills Test Lab 1 m...	SUCCESS	Name: \Users\Administr...
2:39:3...	unpacked_file.exe	3896	Load Image	C:\Users\Administrator\Desktop\COS20030_S2_2023 - Skills Test Lab 1 m...	SUCCESS	Image Base: 0x4a0000, ...
2:39:3...	unpacked_file.exe	3896	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x774a000...
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Users\Administrator\Desktop\COS20030_S2_2023 - Skills Test Lab 1 m...	SUCCESS	Desired Access: Execut...
2:39:3...	unpacked_file.exe	3896	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x763c000...
2:39:3...	unpacked_file.exe	3896	Load Image	C:\Windows\System32\advapi32.dll	SUCCESS	Image Base: 0x7616000...
2:39:3...	unpacked_file.exe	3896	Load Image	C:\Windows\System32\rpcrt4.dll	SUCCESS	Image Base: 0x7728000...
2:39:3...	unpacked_file.exe	3896	Load Image	C:\Windows\System32\msvcrt.dll	SUCCESS	Image Base: 0x764f000...
2:39:3...	unpacked_file.exe	3896	Load Image	C:\Windows\System32\user32.dll	SUCCESS	Image Base: 0x7716000...
2:39:3...	unpacked_file.exe	3896	Load Image	C:\Windows\System32\gdi32.dll	SUCCESS	Image Base: 0x764a000...
2:39:3...	unpacked_file.exe	3896	Load Image	C:\Windows\System32\ws2_32.dll	SUCCESS	Image Base: 0x765f000...
2:39:3...	unpacked_file.exe	3896	Load Image	C:\Windows\System32\nsi.dll	SUCCESS	Image Base: 0x775e000...
2:39:3...	unpacked_file.exe	3896	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	REPARSE	Desired Access: Read
2:39:3...	unpacked_file.exe	3896	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	Desired Access: Read
2:39:3...	unpacked_file.exe	3896	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSAppCompat	NAME NOT...	Length: 548
2:39:3...	unpacked_file.exe	3896	RegQueryValue	HKLM\System\CurrentControlSet\Control\Terminal Server\TSUserEnabled	SUCCESS	Type: REG_DWORD, L...
2:39:3...	unpacked_file.exe	3896	RegCloseKey	HKLM\System\CurrentControlSet\Control\Terminal Server	SUCCESS	
2:39:3...	unpacked_file.exe	3896	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	Desired Access: Read
2:39:3...	unpacked_file.exe	3896	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Lea...	NAME NOT...	Length: 144
2:39:3...	unpacked_file.exe	3896	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon	SUCCESS	
2:39:3...	unpacked_file.exe	3896	RegOpenKey	HKLM\System\Setup	SUCCESS	Desired Access: Read
2:39:3...	unpacked_file.exe	3896	RegQueryValue	HKLM\SYSTEM\Setup\SystemSetupInProgress	SUCCESS	Type: REG_DWORD, L...
2:39:3...	unpacked_file.exe	3896	RegCloseKey	HKLM\SYSTEM\Setup	SUCCESS	
2:39:3...	unpacked_file.exe	3896	RegOpenKey	HKLM	SUCCESS	Desired Access: Maximu...
2:39:3...	unpacked_file.exe	3896	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics	NAME NOT...	Desired Access: Read
2:39:3...	unpacked_file.exe	3896	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query ...
2:39:3...	unpacked_file.exe	3896	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query ...
2:39:3...	unpacked_file.exe	3896	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearch...	NAME NOT...	Length: 16
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Access: Read A...
2:39:3...	unpacked_file.exe	3896	QueryBasicInfor...	C:\Windows\System32\imm32.dll	SUCCESS	CreationTime: 1/9/2022 ...
2:39:3...	unpacked_file.exe	3896	CloseFile	C:\Windows\System32\imm32.dll	SUCCESS	
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Access: Read D...

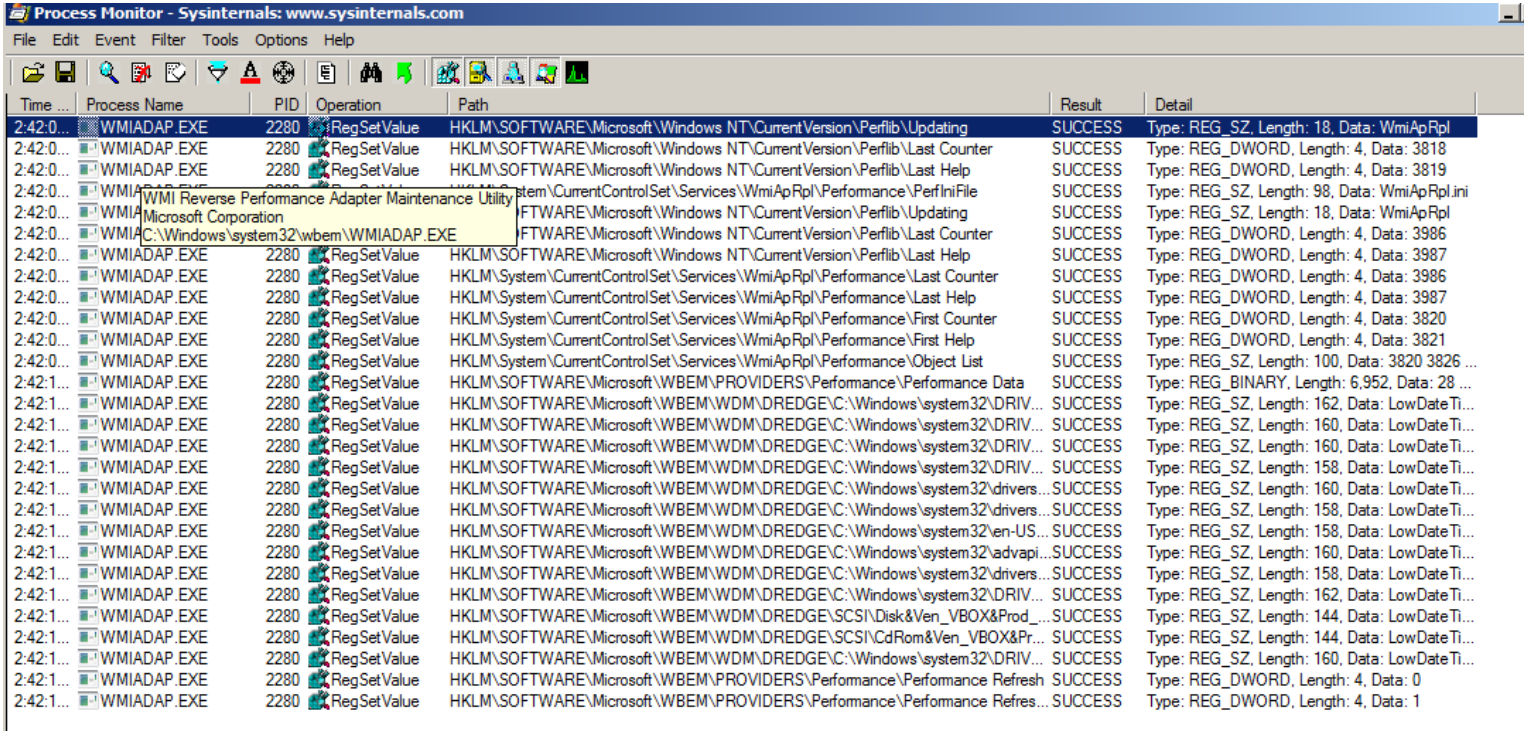
Showing 809 of 532,354 events (0.15%) | Backed by virtual memory

At Process Monitor users can see unpacked_file.exe running even though it doesn't show in Process Explorer.



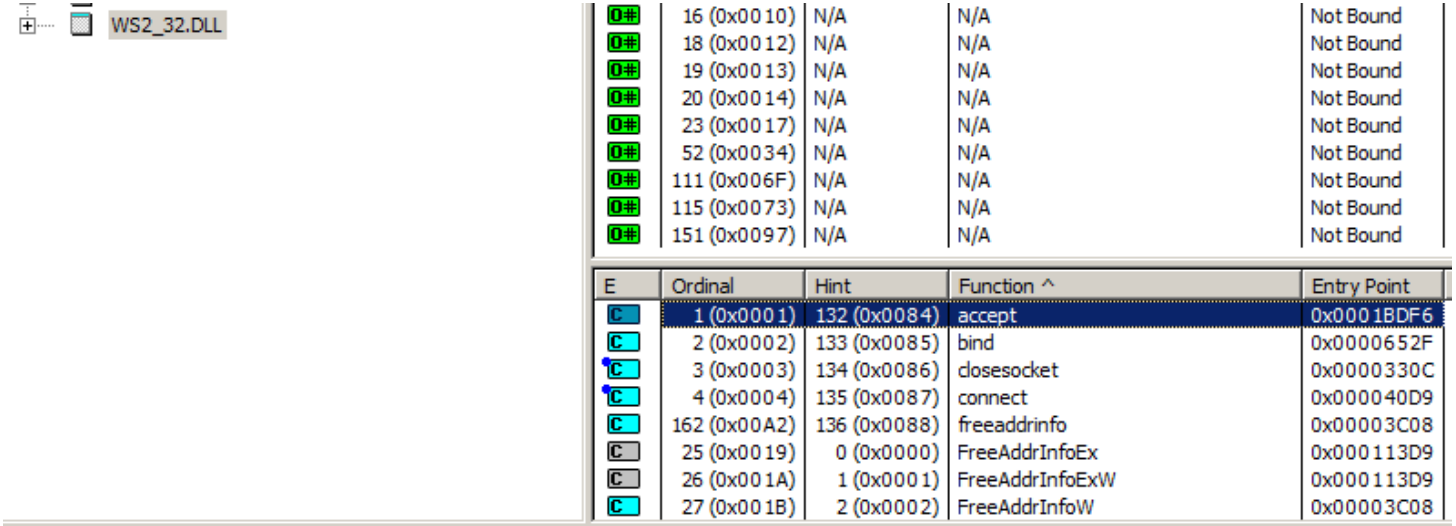
Time ...	Process Name	PID	Operation	Path	Result	Detail
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Users\Administrator\Desktop\COS20030_S2_2023 - Skills Test Lab 1 m...	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\imm32.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\WSHTCPIP.DLL	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\WSHTCPIP.DLL	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\WSHTCPIP.DLL	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\WSHTCPIP.DLL	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\WSHTCPIP.DLL	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\WSHTCPIP.DLL	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wship6.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wship6.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wship6.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wship6.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wship6.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wship6.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\wshqos.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\nlasvc.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\nlasvc.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\NapiNSP.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\NapiNSP.dll	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\WSHTCPIP.DLL	SUCCESS	Desired Acce
2:39:3...	unpacked_file.exe	3896	CreateFile	C:\Windows\System32\WSHTCPIP.DLL	SUCCESS	Desired Acce

Filter the option to CreateFile and the user could see that it has created quite many files.



Time ...	Process Name	PID	Operation	Path	Result	Detail
2:42:0...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Updating	SUCCESS	Type: REG_SZ, Length: 18, Data: WmiApRpl
2:42:0...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Last Counter	SUCCESS	Type: REG_DWORD, Length: 4, Data: 3818
2:42:0...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Last Help	SUCCESS	Type: REG_DWORD, Length: 4, Data: 3819
2:42:0...	WMIA			stem\CurrentControlSet\Services\WmiApRpl\Performance\PerfIniFile	SUCCESS	Type: REG_SZ, Length: 98, Data: WmiApRpl.ini
2:42:0...	WMIA			FTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Updating	SUCCESS	Type: REG_SZ, Length: 18, Data: WmiApRpl
2:42:0...	WMIA			FTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Last Counter	SUCCESS	Type: REG_DWORD, Length: 4, Data: 3986
2:42:0...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib\Last Help	SUCCESS	Type: REG_DWORD, Length: 4, Data: 3987
2:42:0...	WMIADAP.EXE	2280	RegSetValue	HKLM\System\CurrentControlSet\Services\WmiApRpl\Performance\Last Counter	SUCCESS	Type: REG_DWORD, Length: 4, Data: 3986
2:42:0...	WMIADAP.EXE	2280	RegSetValue	HKLM\System\CurrentControlSet\Services\WmiApRpl\Performance\Last Help	SUCCESS	Type: REG_DWORD, Length: 4, Data: 3987
2:42:0...	WMIADAP.EXE	2280	RegSetValue	HKLM\System\CurrentControlSet\Services\WmiApRpl\Performance\First Counter	SUCCESS	Type: REG_DWORD, Length: 4, Data: 3820
2:42:0...	WMIADAP.EXE	2280	RegSetValue	HKLM\System\CurrentControlSet\Services\WmiApRpl\Performance\First Help	SUCCESS	Type: REG_DWORD, Length: 4, Data: 3821
2:42:0...	WMIADAP.EXE	2280	RegSetValue	HKLM\System\CurrentControlSet\Services\WmiApRpl\Performance\Object List	SUCCESS	Type: REG_SZ, Length: 100, Data: 3820 3826 ...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\PROVIDERS\Performance\Performance Data	SUCCESS	Type: REG_BINARY, Length: 6,952, Data: 28 ...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\C:\Windows\system32\DRIV...	SUCCESS	Type: REG_SZ, Length: 162, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\C:\Windows\system32\DRIV...	SUCCESS	Type: REG_SZ, Length: 160, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\C:\Windows\system32\DRIV...	SUCCESS	Type: REG_SZ, Length: 160, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\C:\Windows\system32\DRIV...	SUCCESS	Type: REG_SZ, Length: 158, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\C:\Windows\system32\drivers...	SUCCESS	Type: REG_SZ, Length: 160, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\C:\Windows\system32\drivers...	SUCCESS	Type: REG_SZ, Length: 158, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\C:\Windows\system32\en-US...	SUCCESS	Type: REG_SZ, Length: 158, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\C:\Windows\system32\advapi...	SUCCESS	Type: REG_SZ, Length: 160, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\C:\Windows\system32\drivers...	SUCCESS	Type: REG_SZ, Length: 158, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\C:\Windows\system32\DRIV...	SUCCESS	Type: REG_SZ, Length: 162, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\SCSI\Disk&Ven_VBOX&Prod_...	SUCCESS	Type: REG_SZ, Length: 144, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\SCSI\CdRom&Ven_VBOX&Pr...	SUCCESS	Type: REG_SZ, Length: 144, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\WDM\DREDGE\C:\Windows\system32\DRIV...	SUCCESS	Type: REG_SZ, Length: 160, Data: LowDateTi...
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\PROVIDERS\Performance\Performance Refresh	SUCCESS	Type: REG_DWORD, Length: 4, Data: 0
2:42:1...	WMIADAP.EXE	2280	RegSetValue	HKLM\SOFTWARE\Microsoft\WBEM\PROVIDERS\Performance\Performance Refres...	SUCCESS	Type: REG_DWORD, Length: 4, Data: 1

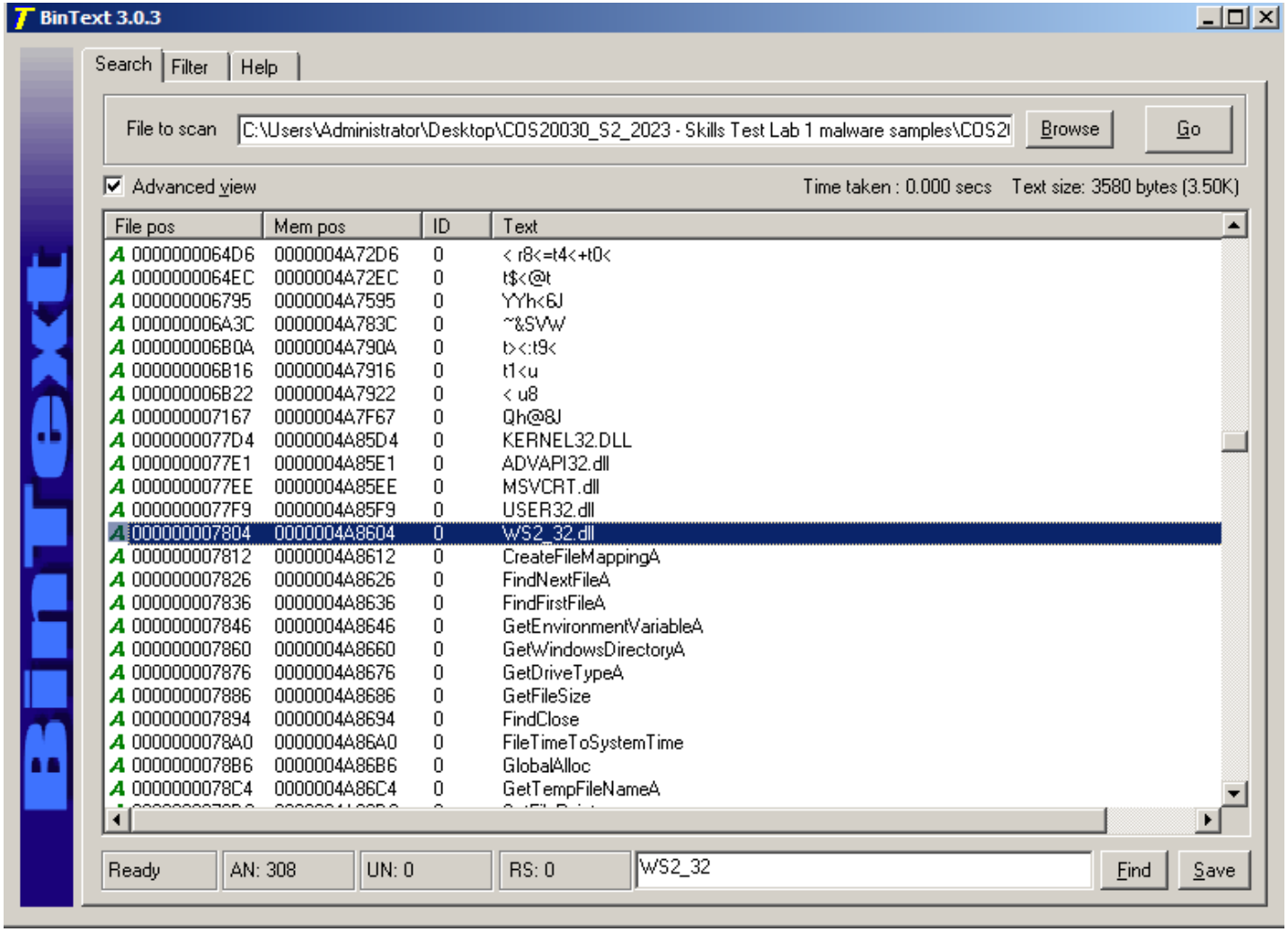
Filter the option for RegSetValue now that the user can see that the registry key that had been created.

<table>
<tr>
<td>Network-based indicators</td>
<td>


O#	16 (0x0010)	N/A	N/A	Not Bound
O#	18 (0x0012)	N/A	N/A	Not Bound
O#	19 (0x0013)	N/A	N/A	Not Bound
O#	20 (0x0014)	N/A	N/A	Not Bound
O#	23 (0x0017)	N/A	N/A	Not Bound
O#	52 (0x0034)	N/A	N/A	Not Bound
O#	111 (0x006F)	N/A	N/A	Not Bound
O#	115 (0x0073)	N/A	N/A	Not Bound
O#	151 (0x0097)	N/A	N/A	Not Bound

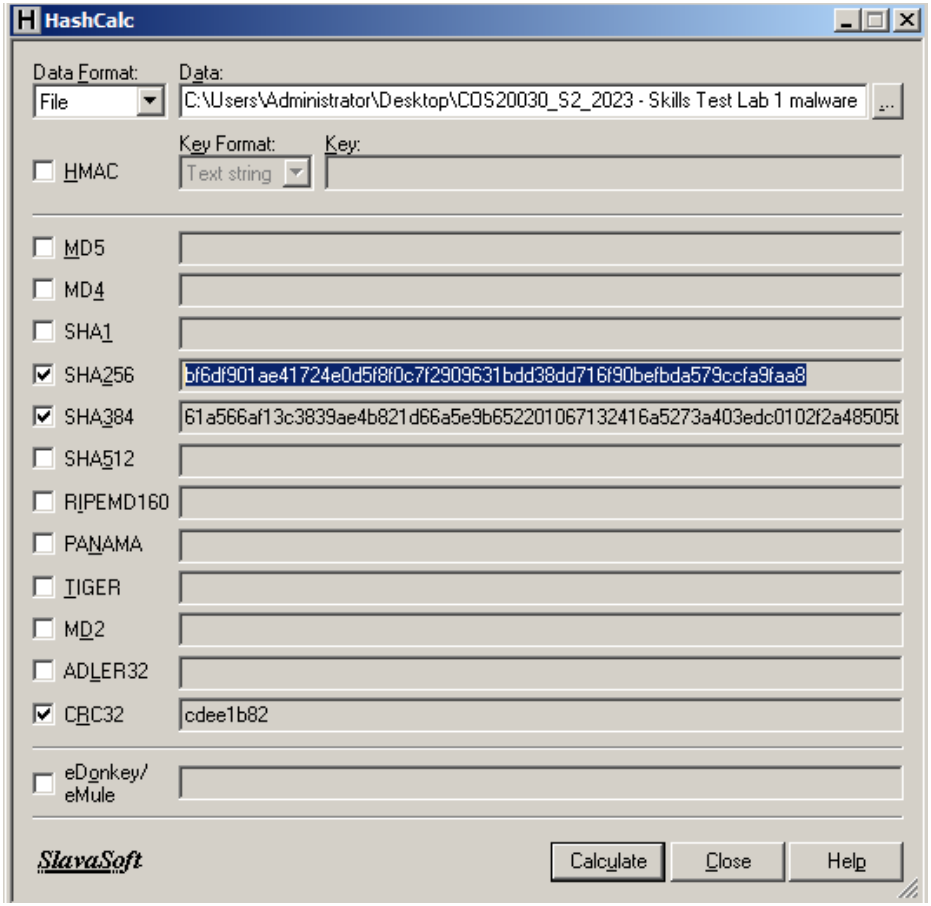
E	Ordinal	Hint	Function ^	Entry Point
C	1 (0x0001)	132 (0x0084)	accept	0x0001BDF6
C	2 (0x0002)	133 (0x0085)	bind	0x0000652F
C	3 (0x0003)	134 (0x0086)	closesocket	0x0000330C
C	4 (0x0004)	135 (0x0087)	connect	0x000040D9
C	162 (0x00A2)	136 (0x0088)	freeaddrinfo	0x00003C08
C	25 (0x0019)	0 (0x0000)	FreeAddrInfoEx	0x000113D9
C	26 (0x001A)	1 (0x0001)	FreeAddrInfoExW	0x000113D9
C	27 (0x001B)	2 (0x0002)	FreeAddrInfoW	0x00003C08

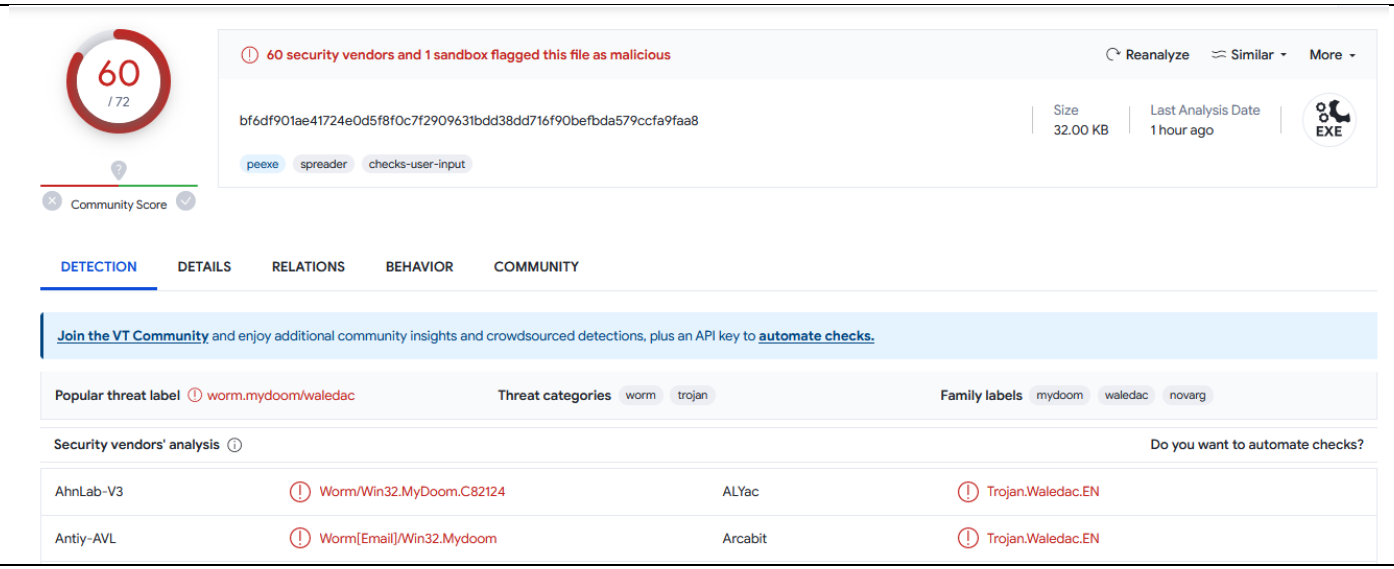
Dependency Walker shows that the export of WS2_32.DLL has accept, bind, and connect. These are supposedly the standard Socket functions used for networking. This suggests that the malware was performing network functions, such as connecting to server and opening a listening port.
</td>
<td>Dependency Walker, BinText</td>
</tr>
</table>



In BinText, the user could also see WS2_32.DLL.

Potential purpose of these files	The.exe file typically performs specialized functions such file manipulation, system administration, memory handling, registry interaction, and text processing as a versatile Windows application. It can manage system processes and threads, a lot and deallocate memory, interface with the Windows Registry for configuration or settings, handle text data, and maybe conduct network communication via socket programming. It can also create, copy, delete, read, and write files. In conclusion, it is a flexible application made for a variety of system-related tasks, making it potentially helpful for jobs ranging from simple file administration to more difficult system and network operations. Based in the information at VirusTotal by HashCal to get the SHA256 and search it in VirusTotal, it seems that it is a threat of worm and trojan.	HashCalc, VirusTotal


HashCalc
Data Format:
File
Data:
C:\Users\Administrator\Desktop\COS20030_S2_2023 - Skills Test Lab 1 malware
Key Format:
Text string
Key:
HMAC
MD5
MD4
SHA1
SHA256
bf6df901ae41724e0d5f8f0c7f2909631bdd38dd716f90befbda579ccfa9faa8
SHA384
61a566af13c3839ae4b821d66a5e9b652201067132416a5273a403edc0102f2a48505b
SHA512
RIPEMD160
PANAMA
TIGER
MD2
ADLER32
CRC32
cdee1b82
eDonkey/
eMule
SlavaSoft
Calculate
Close
Help

** Expand the table if necessary*

(6 marks)

Question 2

You are given an executable file named "sample_q2.exe". This time, you need to perform *dynamic analysis* using tools such as Process Explorer, Process Monitor, and Wireshark.

Document your findings in the table below. Include screenshots where necessary.

Filename: sample_q2.exe		
Analysis	**Description/explanation**	**Tool used**
Host-based indicators	Process Monitor: 1:15:3... sample_q2.exe 3124 Process Create C:\Windows\system32\wscript.exe SUCCESS PID: 2864, Command line: wscript //B C:\Users\ADMINI~1\AppData\Local\Temp\pin.vbs "C:\ProgramData\Microsoft\Windows\Start Menu\Programs\A 1:15:3... wscript.exe 2864 Process Start SUCCESS Parent PID: 3124, Command line: wscript //B C:\Users\ADMINI~1\AppData\Local\Temp\pin.vbs "C:\ProgramData\Microsoft\Windows\Start Menu\Prog Based on above screenshot, we can see that an executable file called "wscript.exe" is being created by sample_q2.exe by using command line through command prompt. The exe file is immediately started after being created 1:15:3... rhcru8j0eee4.exe 576 RegOpenKey HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\pphcvu8j0eee4.e 1:15:3... rhcru8j0eee4.exe 576 Process Create C:\Windows\system32\pphcvu8j0eee4.exe 1:15:3... pphcvu8j0eee4... 3252 Process Start 1:15:3... pphcvu8j0eee4... 3252 Thread Create Based on above screenshot, pphhcvu8j0eee4.exe is being opened through RegOpenKey by its parent exe through imagine file execution options. It is then being launched by its parent. That is how the child exe spam the images as shown in below screenshot:	Process monitor, process explorer


Antivirus XP 2008
Registration
Support
Scan
System Status
Options
Update
About
Realtime Protection
Known viruses : 102563
Scan
Start Scan
Stop Scan
Remove Viruses
Alert ! Your system is infected!
Infected: 412
Antivirus XP 2008
Antivirus XP 2008 has found 412 threats. It is recommended to proceed with removal.
Yes
No
Severity
Status
Win32/IRCBot.AAH
The IRCBot.AAH malware family is a group of bot ...
Win32/Adware.Sear...
Program is used to direct a browser to display pop-...
Win32/Adwre.Virtum...
Virus applications used to deliver advertisements t...
Get Maximal Realtime Protection with Antivirus XP 2008
Antivirus XP 2008 demo mode notice
Antivirus XP 2008
This Computer is infected with spyware and adware
ALERT
Spyware programs install keyloggers, steal credit card numbers and bank information details. This computer can be used for sending spam and you will get popups with adult conten. If you homepage was changed or you have strange popups- this is a sure that your computer is infected
Registration
REGISTER
met Settings\User Agent\Post Platform
met Settings\User Agent\Post Platform\AntivirXP08
Image File Execution Options\pphcvu8j0eee4.exe
ZSXEFV

	Process Explorer: rhcru8j0eee4.exe < 0.01 31,148 K 28,184 K 576 pphcvu8j0eee4.exe < 0.01 1,480 K 4,508 K 3252 An executable file with a strange name is running as it is running another executable file with different strange name Mutant \Sessions\1\BaseNamedObjects\oleacc-msaa-loaded Based on above screenshot, a mutext called “oleacc-msaa-loaded” which is well known mutant to then possibly logs keystrokes from the computer as according to internet rhcru8j0eee4.exe < 0.01 30,036 K 25,600 K 2016 pphcvu8j0eee4.exe < 0.01 1,308 K 4,348 K 964 procexp.exe 2.99 11,816 K 16,924 K 2460 Sysinternals Process Explorer According to above screenshot, when the vm restarted, the two exe are begin there as well.	
Network-based indicators	Process Explorer: ws2_32.dll Windows Socket 2.0 32-Bit DLL Microsoft Corporation C:\Windows\System32\ws2_32.dll wship6.dll Winsock2 Helper DLL (TL/IPv6) Microsoft Corporation C:\Windows\System32\wship6.dll WSHTCPIP.DLL Winsock2 Helper DLL (TL/IPv4) Microsoft Corporation C:\Windows\System32\WSHTCPIP.DLL Based on above screenshot, there are two networking .dll which are ws2_32.dll and WSHTCPIP.dll that could be used for malware to perform network-related task. Process Monitor: 1:20:3... rhcru8j0eee4.exe 576 Load Image C:\Windows\System32\mswsock.dll SUCCESS 1:20:3... rhcru8j0eee4.exe 576 Load Image C:\Windows\System32\mswsock.dll SUCCESS 1:20:3... rhcru8j0eee4.exe 576 Load Image C:\Windows\System32\WSHTCPIP.DLL SUCCESS 1:20:3... rhcru8j0eee4.exe 576 Load Image C:\Windows\System32\WSHTCPIP.DLL SUCCESS Image Base: 0x7 1:20:3... rhcru8j0eee4.exe 576 Thread Create SUCCESS Thread ID: 2472 1:15:4... rhcru8j0eee4.exe 576 Load Image C:\Windows\System32\ws2_32.dll Based on above screenshot, the executable file load image by downloading the image through the networking .dll called WSHTCPIP.dll. As it indicate that it has access to network.	Process explore, process, Wireshark

1:20:3...	rhcru8j0eee4.exe	576	RegCreateKey	HKCU\Software\Microsoft\windows\CurrentVersion\Internet Settings	SUCCESS Desired Acc
1:20:3...	rhcru8j0eee4.exe	576	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\MigrateProxy	SUCCESS Type: REG
1:20:3...	rhcru8j0eee4.exe	576	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable	SUCCESS Type: REG_DWORD, Le
1:20:3...	rhcru8j0eee4.exe	576	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyServer	SUCCESS Type: REG_SZ, Length:
1:20:3...	rhcru8j0eee4.exe	576	RegSetValue	HKLM\System\CurrentControlSet\Hardware Profiles\0001\Software\Microsoft\windows\CurrentVersion\Internet Settings\ProxyEnable	SUCCESS Type: RE

Based on above screenshot, RegSetvalue registry key is being used

1:20:3...	rhcru8j0eee4.exe	576	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings	SUCCESS Type: REG_BINARY, Length: 332, Data: 46 00 00

Wireshark:

dns

No.	Time	Source	Destination	Protocol	Leng	Info
4	1.504822	10.0.2.15	8.8.8.8	DNS	77	Standard query 0x54ed A ocsp.digicert.com
5	1.525116	8.8.8.8	10.0.2.15	DNS	182	Standard query response 0x54ed A ocsp.digicert.com CNAME ocsp.ec
28	2.016299	10.0.2.15	8.8.8.8	DNS	86	Standard query 0x9d10 PTR 76.38.195.152.in-addr.arpa
29	2.048507	8.8.8.8	10.0.2.15	DNS	157	Standard query response 0x9d10 No such name PTR 76.38.195.152.in
47	431.05…	10.0.2.15	8.8.8.8	DNS	84	Standard query 0xc567 A www.antivirusxp-2008.com
48	431.08…	8.8.8.8	10.0.2.15	DNS	157	Standard query response 0xc567 No such name A www.antivirusxp-20
53	532.34…	10.0.2.15	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
54	532.38…	8.8.8.8	10.0.2.15	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.
55	551.45…	10.0.2.15	8.8.8.8	DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
56	551.47…	8.8.8.8	10.0.2.15	DNS	104	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR dns.
57	551.47…	10.0.2.15	8.8.8.8	DNS	82	Standard query 0x0002 PTR 15.2.0.10.in-addr.arpa
58	551.51…	8.8.8.8	10.0.2.15	DNS	82	Standard query response 0x0002 No such name PTR 15.2.0.10.in-add

Based on above screenshot, we can see there are DNS lookup for different domain such as digicert.com, anitvirusxp-2008.com or PTR in every once in a while, but all of their IP address are same. It is an indicative of network-based as such technique of changing domain name but with consistent IP address is often used by malware attacker that is called as domain generation algorithm to evade detection by generate different name as according to internet.

Potential purpose of these files	Purpose of all these files are that the malware change the proxy settings and the use of several networking .dllthrough registry to establish contact with its host. It is possible that the malware is collecting information and sending it to its host	

** Expand the table if necessary*

(4 marks)